Department of Digital Systems

Postgraduate Programme “Digital Systems Security”

Master’s Thesis

Cybersecurity Education Status and Curriculum Analysis

Smaili Efthimia

MTE1826

Supervisor

Ntantogian Christoforos

February 2021

Table of Contents

1. Introduction

This dissertation examines the current state of the cybersecurity education status and curriculum in order to improve the general understanding of the rationale for choosing a cybersecurity approach. More specifically, the goal is to study the existing resources as master's degrees, online trainings and certifications and identify their focus, whether it is offensive, defensive or both.

The offensive approach is represented by the Red Teams. Red Team is a wide discipline that applies to many fields: intelligence, business, national security and cybersecurity [1]. In cybersecurity, Red Teams are external entities brought in an organization to test the effectiveness of a security program. They are hired to emulate the behavior and techniques of attackers to make the campaign as realistic as possible. Red team goals testify the ability of an attacker to violate confidentiality, integrity or availability of a vulnerable system. Typical objectives are service disruption, exfiltration of sensitive data, stealthy movement across systems [2]. In addition to finding un-patched vulnerabilities one of the most important objectives of a red team is evaluating the organization's security readiness, active controls, and countermeasures by emulating a full attack cycle [3].

The defensive approach is represented by the Blue Teams which are the defensive teams that should stop simulated attacks, and carry out response actions such as investigations and security remedies. For an organization, the goal is to get a realistic evaluation of its defensive capabilities by seeing how their security teams with different levels of preparation react to the simulation [2]. The blue team is responsible to identify and patch potential vulnerabilities that can be exploited by a red team [4].

Purple Team describes more often the collaboration of red and blue teams than a standalone team.

Analyzing the Cybersecurity Education Status and Curriculum is essential to understanding why there is a tendency towards red, blue or purple teaming. However, there is a lack of scientific publications which study this matter. Fill such a gap is the primary driver of this research.

2. Research results

In the context of this dissertation, cybersecurity related master's degrees were researched as well as the training courses available in the massive open online course provider Udemy and security certifications mainly applicable for red and blue teaming. The goal was to identify the focus of the existing training resources.

2.1. Methodology

Regarding the research of master's degrees, the in-scope programs were those of the cybersecurity, information security, computer security, information technology security, software security, information assurance, software security, digital forensics, resilience, threat intelligence, ethical hacking and penetration testing domains. Programs with main focus on domains such as risk management and data protection and privacy were not included. Regarding the geographical scope, no countries were excluded, however, only the programs with syllabus available in English are encompassed. The programs' modules where categorized based on their subject in "Red Team" category, which relates to courses with focus on attacks, "Blue Team" category, which relates to courses with focus on defense and "Generic" category, which relates to security courses that do not appertain to either of the aforementioned categories. Modules with no security content were omitted.

With regards to the Udemy courses, the range of the research covered the "Network & Security" category which breaks down in "Ethical Hacking", "Cyber Security", "Network Security" and "Penetration Testing" categories. From those, courses correlated with certification preparation were excluded as well as risk management, business continuity and disaster recovery and data protection and privacy. All lessons taken into account were in English and with duration over than one hour. In this case, the courses were categorized based on their content in "Red Team" and "Blue Team", with the same rationale as above, and in "Purple Team" in case the subject introduced combined both.

Apropos of the security certifications, the in-scope programs were mostly of the Security Operations domain which includes Forensics, Incident Handling, Penetration Testing and Exploitation certifications. In addition, certifications regarding Network Security but with a defined content with reference to defending the network, such as firewalls, were incorporated. All involved certifications required either theoretical or practical exams, courses that resulted to issuing a certification of attendance were not taken into account. In like manner, the certifications were categorized based on their content in "Red Teams", for the Penetration Testing and Exploitation domain, in "Blue Teams", for the Forensics and Incident Handling domain and those with regarding firewalls and SIEMs, and in "Purple Team" in case the content combined both.

2.2. Research results

2.2.1. Master's Degrees

For the purpose of this dissertation 1644 modules of 195 courses from 176 Universities were reviewed in a worldwide scope. Each course's modules were classified based on the focus of the module in "Red Team", "Blue Team" and "Generic" categories. The detailed results can be found in the following link and the aggregated results are presented in the table below:

Table 1. Master's Degrees Modules Categorization Results

Category	Count of Modules
Red Team	184
Blue Team	333
Generic	1127

According to research results, 184 modules were classified as "Red Team", meaning that the main focus was on practical attacking concepts. Indicative modules that were integrated in this category are:

- Penetration Testing,
- Malware Analysis,
- Ethical Hacking,
- Reverse Program Engineering,
- Malware Reverse Engineering,
- Python for penetration testing,
- Embedded System Hacking and Security,
- Social Engineering,
- Web application penetration testing,
- Cyber Warfare and Cyber Crime,
- Red Teaming,
- Hardware-Level Cyber Security,
- Side-Channel Attacks and Modern Cryptanalysis.

333 modules were classified as "Blue Team", meaning that the main focus was on practical defensing concepts. Indicative modules that were integrated in this category are:

- Digital Forensics,
- Kernel Forensics and Analysis,
- Forensic Auditing for Computing Security,
- Cyber Threat Intelligence,
- Information Systems Auditing,
- Engineering Resilient Systems,

- Incident Management and Response,
- Security Operations Center (SOC) & Incident Response,
- Digital Investigation and Evidence Management,
- Intrusion detection and response,
- Firewall and IPS Technology,
- Investigating Online Crimes,
- Fraud Examination,
- Protection Against Specific Cloud Threats,
- Proactive network defense,
- Enterprise continuity & recovery planning,
- Malware Defenses and Application Security,
- SIEM/CDC,
- Methods for attacks detection.

1127 modules were classified as "Generic", meaning that the main focus was not of the defense nor the attack concept, but of general cybersecurity domains. Indicative modules that were integrated in this category are:

- Network Security,
- Communications Security,
- Computer Security,
- Software Security,
- Data Security,
- IoT Security,
- Cloud Security,
- Security Management,
- Risk Management,
- Cryptography,
- Cyber Law,
- Privacy,
- Legal and Regulatory Framework of Security,
- Ethics.

Delving into indicative master's degree programs, initially, an analysis on Johns Hopkins Whiting School of Engineering (Baltimore, Maryland) Master of Science in Cybersecurity curriculum is presented. Of a total of 20 cybersecurity related modules, 3 were classified as "Red Team", 4 as "Blue Team" and 13 as "Generic".

The "Red Team" modules include Introduction to Ethical Hacking and Reverse Engineering and Vulnerability Analysis. Introduction to Ethical Hacking module's goal is to make students familiar with computer hacking and help them comprehend how to attack vulnerable systems via hands-on assignments. Reverse Engineering and Vulnerability Analysis focuses on discovering software vulnerabilities, examining threats and practicing passive and active reverse engineering techniques by using static analysis, dynamic reverse engineering tools, and fault injection via fuzzing.

The “Blue Teams” modules include Computer Forensics, Intrusion Detection, Digital Forensics Technologies and Techniques and Embedded Computer Systems-Vulnerabilities, Intrusions, and Protection Mechanisms. Computer Forensics focuses on techniques and tools to identify, collect, examine and preserve information from digital equipment. The computer forensics tools are used to gain a thorough understanding of the processes and techniques used in acquiring information and evidence. Intrusion Detection introduces Intrusions Detection Systems and analyzes approaches, models, algorithms and practical concerns of IDS solutions. In addition, false positives and missed detection tradeoffs are examined. TCPDump and Snort are used for the assignments. Digital Forensics Technologies and Techniques exposes students to the acquisition, identification, attribution, and analysis of digital evidence of an event occurring in a computer or network and in particular in signature extraction techniques, detection, classification and retrieval of forensically interesting patterns. In addition, Antiforensic techniques will be examined using programming practice through case studies. Finally, Embedded Computer Systems-Vulnerabilities, Intrusions, and Protection Mechanisms provides understanding of embedded computer systems: differences with respect to network-based computers, programmability, exploitation methods, and current intrusion protection techniques, along with material relating to computer hacking and vulnerability assessment.

The “Generic” modules include Foundations of Information Assurance, Cryptology, Information Assurance Analysis, Intelligent Vehicles: Cybersecurity for Connected and Autonomous Vehicles, Survey of Cloud Computing Security, Public Key Infrastructure and Managing E-Security, Web Security, Network Security, Information Assurance Architectures and Technologies, Security and Privacy in Computing, Operating Systems Security, Security Engineering, Java Security, and Authentication Technologies. Foundations of Information Assurance targets on identifying threats to enterprise information technology systems, access control and open systems, and system and product evaluation criteria. In addition, the module covers topes such as network security, cryptography, IT technology issues, database security, access control (hardware and software), communications security, the proper use of system software (operating system and utilities) and social and legal problems of individual privacy. Cryptology introduces the concept of classical cryptography techniques and contemporary cryptology: symmetric block ciphers and the Advanced Encryption Standard, public key cryptosystems, digital signatures, authentication protocols, cryptographic hash functions, and cryptographic protocols and their applications. Information Assurance Analysis focuses on the analysis process and approach rather than on specific tools. The analysis process includes the collection, use, and presentation of data from a variety of sources, which are used by a variety of analytical techniques, such as collection approach evaluation, population estimation, hypothesis testing, experiment construction and evaluation, and constructing evidence chains for forensic analysis. Intelligent Vehicles: Cybersecurity for Connected and Autonomous Vehicles elaborates the magnitude of security and on smart vehicles, teaches experimental design and the scientific method. Survey of Cloud Computing Security analyzes the security concerns and countermeasures for a cloud environment, access control in the cloud, identity management, denial of service, account and service hijacking, secure APIs, malware, forensics, regulatory compliance, trustworthy

computing, and secure computing in the cloud. Public Key Infrastructure and Managing E-Security focuses on public key technology and related security management issues in the context of the Secure Cyberspace Grand Challenge of the National Academy of Engineering. The module analyzes PKI related concept such as public key technology, digital certificates, certificate policy and certification practices, identification challenges and key management lifecycle process. Web Security examines the protection of connections between a client and server using current encryption protocols, data privacy and elementary number theory. Network Security, apart from security architecture matters, incorporates applied cryptography and information security e.g. encryption algorithms, hash algorithms, message integrity checks, digital signatures, security assessment and authentication, authorization and accounting (AAA), security association, and security key management (generation, distribution, and renewal). Information Assurance Architectures and Technologies examines, among others, layered security architecture guidance and cases, cryptographic commercial issues, hypervisor and cloud computing security architecture, and information assurance architectures technologies applications. Security and Privacy in Computing covers fundamental principles of building secure systems and techniques to ensure data security and privacy as access control mechanisms, operating systems security, malicious code threats and software security, trusted computing, content protection, and database security. Operating Systems Security examines, among others, access control mechanisms, memory protections, inter-process communications mechanisms, policies designed to help protect systems against sophisticated attacks, advanced persistent threats, including rootkits and malware protection mechanisms designed to refute these types of malicious activities. Security Engineering covers the principles of cybersecurity design and engineering, cybersecurity risk assessment, intrusion detection design. Java Security covers security concepts as confidentiality, integrity, authentication, access control, and nonrepudiation in the context of Java language, cmobile code, mechanisms for building “sandboxes”, symmetric and asymmetric data encryption, hashing, digital certificates, signature and MAC generation/verification, code signing, key management, SSL, and object-level protection. Authentication Technologies targets on multi-factor authentication technologies, evaluation of authentication processes, practical issues of authentication, password cracking techniques, key logging, phishing, and man-in-the-middle attacks authentication breaches and ethical hacking techniques.

Abertay University’s (Dundee, Scotland) Ethical Hacking and Cyber Security Master’s Degree is a one-year program which includes 5 cybersecurity related modules, 1 of them is classified as “Red Team”, 2 as “Blue Team” and 2 as “Generic”.

The “Red Team” module is Ethical Hacking 4 which, according to module’s curriculum, exposes students to advanced hacking techniques and their countermeasures. The “Blue Team” modules are Digital Forensics 3 and Engineering Resilient Systems 1. Digital Forensics 3 teaches students how to perform and evaluate computer forensic investigations and forensic software in order to develop appropriate investigation strategies. Engineering Resilient Systems Masters focuses on Hardware Security Challenges, The Ingredients of Machine Learning, Support Vector Machines for Cyber Security, Neural Networks for Cyber Security, Authentication Design, Principles of

Secure Software Development, Language and API Design for Security, Static and Dynamic Analysis and Insider Threat. The "Generic" modules are Computer Security and Information and Network Security Management. Computer Security provides an introduction to computer security and ethical hacking and a high-level presentation of vulnerability improving and computer defense techniques. Network Security Management targets on the assessment of threats to information systems and the related countermeasures in order to expose students to the architecture and management of computer networks and security implications of architectural structures.

The Master of Science in Cyber Security of Koc University (Istanbul, Turkey) includes 7 cybersecurity related modules, 1 of which is classified as "Red Team", 2 as "Blue Team" and 4 as "Generic".

The "Red Team" module is Applied Penetration Testing which introduces students to penetration testing definitions, white hat attacking methodologies, network and software scanning and inventory tools, exploit tools, social engineering techniques, applied penetration testing software. The "Blue Team" modules are Cyber Forensics and Secure Software Coding and Testing. Cyber Forensics focuses on cyber forensics and digital forensics definitions, evidence collection methodologies, data recovery tools, software and hardware tools employed for forensic analysis, evidence reporting procedures, and techniques. Secure Software Coding and Testing targets on secure coding principles, software testing methodologies, techniques and tools for secure software coding, operating system, and database support for secure software, reverse engineering, techniques for hiding code and data. The "Generic" modules are Computer and Network Security, Modern Cryptography, Internet and Cloud Security and Cybersecurity and Data Protection Law. Computer and Network Security exposes students to computer security techniques, conventional encryption, public-key cryptography, key management, message authentication, hash functions and algorithms, digital signatures, authentication protocols, access control mechanisms, network security practice, TCP/IP Security, web security, SSL (Secure Socket Layer), Denial-of-Service attacks, intrusion detection, viruses. Modern Cryptography teaches students about symmetric encryption, the public-key breakthrough, one-way functions, hash functions, random numbers, digital signatures, zero-knowledge proofs, modern cryptographic protocols, multi-party computation. In addition, the course introduces everyday use examples including online commerce, BitTorrent peer-to-peer file sharing, and hacking some old encryption schemes. Internet and Cloud Security focuses on Network security, Internet and World-Wide Web security, TLS/SSL, firewalls, intrusion detection, and prevention systems, the security of various Internet and cloud protocols, virtual machine security. Finally, Cybersecurity and Data Protection Law target on the legal aspects of cybersecurity, cybercrime, various data privacy regulations (KVKK, GDPR, HIPAA), electronic signature law, comparative legal analysis of national and international cybersecurity law.

Edith Cowan University's (Perth, Western Australia, Australia) Master of Cyber Security is a 2-year program which includes 5 cybersecurity related modules, 1 of them is classified as "Red Team", 1 as "Blue Team" and 3 as "Generic".

The “Red Team” module, Ethical Hacking and Defense, introduces ethical hacking to students focusing on network-enabled services and technologies by learning techniques for evaluating the security of network configuration and to defend against network-based threats. The “Blue Team” module, Digital Forensics, introduces students to digital forensic tools, techniques and methods used to recover and examine digital evidence from electronic devices and teaches how to preserve, identify and analyze digital based evidence acquired from storage locations using specific software tools techniques and processes to recover evidence. The “Generic” modules are Cyber Security, Cyber Security Management and Network Security. Cyber Security introduces cyber security to students by exposing them to threats and vulnerabilities of computer systems, networks and information assets through the examination of countermeasures that can be used to minimize the associated security issues. The concepts covered in this course are risk management and contingency planning, malicious software, authentication and access control, encryption, operating system security, information classification, and privacy. Cyber Security Management analyzes governance, strategy and change management within the context of cyber security on a theoretical and practical level and teaches students how to understand the causes of a cybersecurity problem and design a feasible solution for it. Finally, Network Security focuses on the effective deployment, utilization and monitoring of both wired and wireless networks by exposing students to a wide range of techniques, tools and policies to effectively secure such networks.

Bellevue University’s (Bellevue, Nebraska) Master of Science in Cyber Security includes 16 cybersecurity related modules, 3 of which is classified as “Red Team”, 4 as “Blue Team” and 9 as “Generic”.

The “Red Team” courses are Ethical Hacking and Response, Information Warfare and Advanced Cybersecurity Testing. Ethical Hacking and Response teaches students regarding offensive and defensive techniques for protecting cyber assets, security testing, risk mitigation techniques, threat response, penetration testing theory, techniques, and tools, network, systems, and application vulnerability scanning, risk analysis and response, and intrusion detection and response. Information Warfare provides an overview of the fundamental processes associated with waging war in an electronic age. Topics include strategic planning and tactical analysis for target identification, reconnaissance, and tool selection. The intent of this course is to focus on individual, corporate and national forms of warfare. Advanced Security Testing teaches students how to prepare and conduct penetration tests on computers, networks, and devices using tools and complex methods for exploiting client-side, service side and privilege escalation attacks by using tools, techniques, and technologies for determining vulnerabilities in information systems and applications. The “Blue Team” modules are Computer Forensics, White Collar Crime, Advanced Computer Forensics, Business Continuity and Recovery Planning. Computer Forensics covers processing crime and incident scenes, digital evidence controls, recovery of information, network forensics, data acquisition, and legal and ethical issues associated with investigations. White Collar Crime targets on fraud prevention, anti-money laundering, investigative methodologies, and protecting privacy and allows students to demonstrate real-world scenarios of white collar crimes, how to prevent or deter them, detection methods, and

response techniques. Advanced Computer Forensics exposes students to an advanced study of computer, network, and device forensics by conducting hands-on forensic research to identify how digital media and/or digital networks were compromised and the method(s) of intrusion employed. The course includes the review of what data is stored on a device, how the device services are consumed, and what methods attackers (and forensic analysts) deploy to retrieve information without an owner's permission. Business Continuity and Recovery Planning incudes project scope and planning, assessing risk, developing policy and procedures, conducting business impact analyses, recovery strategies, recovery plan development, implementation, recovery plan development, implementation, and restoration. The "Generic" modules are Information Security Management, Physical, operations and personnel security, Security Architecture and Design, Human Aspects of Cybersecurity, Risk Management Studies, Cybersecurity Governance and Compliance, Introduction to Cyber Ethics, Cyberwar and Cyberdeterrence and Control System Security. Information Security Management includes access control systems, network and software security, management practices, risk management, protection mechanisms, business continuity planning, and legal and ethical issues. Physical, operations and personnel security examines the effective security methodologies based on comprehensive assessment of threats and implementation of a layered system of physical and electronic protection. In addition, threat identification, countermeasures, and prevention are explored. Security Architecture and Design focuses on computer organization, hardware, software and firmware components, open and distributed systems, protection mechanisms, certification and accreditation, formal security models and evaluation criteria. Human Aspects of Cybersecurity targets on understanding human behavior and interaction, motivation and influence, and social engineering. Risk Management Studies exposes students to methodologies and models for managing risks, recognition of security threats and vulnerabilities and the analysis of associated risks. Cybersecurity Governance and Compliance teaches the importance of compliance with laws, regulations, policies, and procedures as a means of minimizing risk through mandated security and control measures. Introduction to Cyber Ethics covers concepts as ethics, computer privacy and security, computer crime and software piracy, intellectual property and information ownership, computers and gender, computers and social justice and civil liberties in cyberspace. Cyberwar and Cyberdeterrence includes aspects of non-state actors, international law, financial flows, and state capabilities. The module also targets on understanding how states try to protect themselves (and develop their own cyber weapons), in addition to comprehending the legal and ethical complications. Finally, Control System Security explores risks associated with Industrial Control Systems (ICS) within and across critical infrastructure and key resource sectors. Topics include a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

2.2.2. Udemy

721 cybersecurity related courses from the massive open online course provider Udemy were reviewed for the purpose of this dissertation. Each course was classified based on its content in "Red Team", "Blue Team" and "Purple Team" categories. The detailed

results can be found in the following link and the aggregated results are presented in the table below:

Table 2. Udemy Courses Categorization Results

Category	Count of Modules
Red Team	483
Blue Team	205
Purple Team	33

According to research results, 483 courses were classified as "Red Team", meaning that the main focus was on practical attacking concepts. Indicative courses that were integrated in this category are:

- Learn Ethical Hacking From Scratch,
- Website Hacking / Penetration Testing & Bug Bounty Hunting,
- A Start-to-Finish Guide to Malware Analysis!: 2-in-1,
- Advanced Ransomware Reverse Engineering,
- Ethical Hacking with Metasploit: Exploit & Post Exploit
- Practical Guide to Penetration Testing with Kali Linux,
- SQL Injection Ethical Hacking Course,
- Bug Bounty Hunting : XSS - Beginner to Advance,
- Cyberhacker Series: Malware Development,
- Practical Hacking: Undetectable Malware,
- Virus, Worm, Trojan, Backdoor & Antivirus-Malware and Security.

205 courses were classified as "Blue Team", meaning that the main focus was on practical defensing concepts. Indicative modules that were integrated in this category are:

- Defeat Viruses! Protection and Prevention Strategies
- Network Safeguard with Fortinet FortiGate Firewall,
- A Guide to Security Information and Event Management – SIEM,
- A Guide to Ransomware Protection,
- Threat Modeling,
- Palo Alto Firewalls - Installation and Configuration,
- Cyber Security Incident Handling and Response,
- Cisco Firepower Threat Defense : Basic Lab Guide,
- Computer Forensics Training: Hands-on Lab,
- Cyber Security Incident Response WannaCry Ransomware,
- Hands On: Azure Sentinel Cloud SIEM & SOAR.

33 courses were classified as "Purple Team", meaning that the main focus was on practical defensing and attacking concepts. Indicative courses that were integrated in this category are:

- Python: Digital Forensics & Binary Exploits with Python,
- Wireless Hacking and Security,
- Hacking and Securing Kubernetes Clusters,
- Practical Cyber Threat Hunting,
- Kali Linux: Network Scanning, Pentesting & Digital Forensic,
- Pentesting and Securing Web Applications.
- Certified Ethical Hacker (CEH),
- GXPN: GIAC Exploit Researcher and Advanced Penetration Tester,
- Offensive Security Certified Professional (OSCP),
- Certified Penetration Testing Engineer C)PTE,
- CREST Certified Malware Reverse Engineer (CCMRE),
- eLearnSecurity Web application Penetration Tester eXtreme eWPTXv2,
- CompTIA Pentest+,
- Certified Red Team Professional.

79 certifications were classified as "Blue Team", meaning that the main focus was on practical defensing concepts. Indicative certifications that were integrated in this category are:

- EC-Council's Certified Incident Handler (ECIH),
- GCFA: GIAC Certified Forensic Analyst,
- GCED: GIAC Certified Enterprise Defender,
- Certified Network Defender CND,
- CREST Practitioner Intrusion Analyst CPIA,
- CREST Practitioner Threat Intelligence Analyst (CPTIA),
- CyberSec First Responder CFR,
- Blue Team Level 2 BTL2,
- IBM Certified SOC Analyst - IBM QRadar SIEM V7.3.2.

3 certifications were classified as "Purple Team", meaning that the main focus was on practical defensing and attacking concepts. The certifications that were integrated in this category are:

- GDAT: GIAC Defending Advanced Threats,
- GCIH: GIAC Certified Incident Handler,
- GREM: GIAC Reverse Engineering Malware.

Delving into indicative courses of the "Red Team" category, initially, an analysis on one of the most popular and highest rated courses, Learn Ethical Hacking From Scratch, is presented. It is a 14,5-hour course which consists of four sections: Network Hacking, Gaining Access, Post exploitation and Website/ Web Application Hacking.

Network Hacking section focuses on how to test the security of wired and wireless networks. This section is further segregated in three sub-sections: pre-connection attacks, which teaches how to attack a network without connecting to it, how to gather information about the network and discover connected devices, gaining access, which teaches students how to use the information gathered in the previous sub-section in order to get the WIFI password, and post connection attacks, which exposes students to

attacks like code injection, creating an evil twin. Gaining Access section describes server-side attacks and client-side attacks. Server-side attacks are launched directly to a server and do not require user interaction and use information as operating system, open ports, installed devices to discover weaknesses and vulnerabilities and exploit them. Client-side attacks require ser interaction and are usually launched when a user downloads malicious content through social engineering. The course introduces how to create trojans by backdooring normal files and use the gathered information to spoof emails. Post exploitation section teaches how to access file systems, maintain access and pivot to other systems. Website / Web Application Hacking exposes students to discovering and exploiting vulnerabilities as file upload, code execution, local file inclusion (LFI), remote file inclusion (RFI), SQL injection and Cross Site Scripting (XSS).

Website Hacking / Penetration Testing & Bug Bounty Hunting is a 9-hour course which teaches students how to become bug bounty hackers. The course consists of three sections: Information Gathering, Discovery, Exploitation & Mitigation and Post Exploitation. Information Gathering section focuses on how to gather information about a website, how to discover DNS information, the used services, subdomains, un-published directories, sensitive files, user emails, websites on the same server and the hosting provider. Discovery, Exploitation & Mitigation teaches students how to discover, exploit and mitigate numerous vulnerabilities and describes the vulnerabilities themselves, what is to be gained, how to bypass security and exploit the vulnerabilities and how to fix them. The included vulnerabilities are: File upload, a vulnerability which allows attackers to upload executable files on the target web server, Code Execution, a vulnerability which allows attackers to execute system code on the target web server, Local File Inclusion, a vulnerability which allows attackers to read files on the target server, Remote File Inclusion, a vulnerability which allows attackers to load remote files, SQL Injection, a vulnerability which may allow attackers to login as admin without knowing the password, access the database and get all data stored there such as usernames and passwords, Cross Site Scripting (XSS), a vulnerability which allows attackers to inject JavaScript code in vulnerable pages and may steal credentials from users, Insecure Session Management, a vulnerability which allows attackers to login to other user accounts and Brute Force & Dictionary Attacks. Finally, Post Exploitation section focuses on how to convert reverse shell access to a Weevely access and vice versa, how to execute system commands on the target server, navigate between directories, access other websites on the same server, upload/download files, access the database, download the whole database and bypass security.

A Start-to-Finish Guide to Malware Analysis!: 2-in-1 is a 6-hour course that teaches dynamic and static malware analysis and the use of OllyDbg, WINDBG, and IDA Pro. The course consists of 2 sections: Fundamentals of Malware Analysis and Advanced Malware Analysis. The first introduces students to various types of malware analysis tools and techniques and the malware analysis process. Students learn basic techniques of static and dynamic malware analysis using debuggers and disassemblers such as OllyDbg and IDA PRO and techniques that malware may use to evade detection and remain undetected. Advanced Malware Analysis teaches about malware behavior and evading it using IDA Pro, OllyDbg, and WINDBG. This section introduces a deep-

down view on advanced malware analysis topics and explores defense mechanisms against malware, create a signature for malware, set up an intrusion detection system (IDS) to prevent attacks and how to unpack packed malware to analyze it.

Advanced Ransomware Reverse Engineering is an 1-hour course which aims to provide a practical approach to analyzing ransomware including topics as: identify and work around anti-virtualization techniques deployed inside malware samples, dynamic analysis of sample's activity on a Windows box, advanced debugging techniques, use static analysis to discover and understand encryption algorithms, discover, and work-around, obfuscation tricks and anti-static analysis tricks, discover flaws that allow us to recover encrypted files, write decryptors in Python and C. The main focus of this course is the Yellow Dragon Ransomware demonstrates dynamic analysis overview and in action, cryptanalysis overview and in action, static analysis overview and in action, data section decryption overview and in action and file recovery overview and in action. Finally, a quiz consisted of 10 questions for students to test their knowledge is provided.

Ethical Hacking with Metasploit: Exploit & Post Exploit is a 5-hour course which teaches how to use Metasploit to exploit vulnerabilities. The course apart from setting up the lab and install the virtual machines and tools introduces some terminology and focuses on how to use Nessus to scan vulnerabilities and gain access to systems. In addition, the students are taught how to use Metasploit framework for compromising systems and demonstrate the Pass the Hash technique. Other techniques included are keylogger, and learn how to crack password hashes using brute force and dictionary attacks. Finally, collection of sensitive data is demonstrated using real world examples.

Scrutinizing the "Blue Team" category, Defeat Viruses! Protection and Prevention Strategies is a 3-hour course which focuses on how to defend against viruses by teaching how to install and set up an antivirus and antimalware program and configuring and implement a backup strategy. The strategies this course introduces as the main ones for defeating viruses and protecting computers and networks are: typical precautions like antivirus and antimalware applications, multi-tiered backup strategy, virtual machines for system isolation, bootable USB flash drive for further system isolation and setting up a secondary PC for online activities.

Network Safeguard with Fortinet FortiGate Firewall is a 5-hour course which teaches students how to install, configure, deploy and fine tune your FortiGate UTM box Initially, the course introduces the basic network configuration, including creating zones, setting up admin accounts, enable features in FortiGate, deploying dashboards and VLANs. In addition, the course focuses on setting the security profile, including the antivirus profile, creating web and DNS filters, application controls and the Intrusion Prevention System. Going forward, the creation of addresses and groups is presented as well as the creation of IPv4 policy, traffic shaping, SD WAN and IP Sec and SSL VPN. FortiGate Firewall also includes user management features as guest management, two-factor authentication (FortiToken) and SMS server configuration to which also apply two-factor authentication. Students can also learn CLI commands, how to monitor threads, identity and correlate events, how to report generation and analysis and how to analyze logs and distinguish anomalies.

A Guide to Security Information and Event Management – SIEM is a 16.5-hour course which provides hands-on experience on Splunk Security information and event management and Security event manager. It covers Navigating Splunk web: Splunk home, Splunk bar, Splunk web, getting date into Splunk, how to specify data inputs, where Splunk stores data, getting tutorial data into Splunk, using Splunk search, search actions and modes, search results tools, events, what are fields, extracted fields, find and select fields, run more targeted searches, use the search language and learn with search assistant. It is consisted of 18 sections, section 1 Introduction to SIEM focuses on a high-level view of Security information and event management and Security event manager. Section 2 Key Objectives of SIEM teaches students how to identify threats and breaches, collect logs and conduct investigations. Section 3 Defense in Depth introduces the multilayered defensive mechanism approach. Section 4 Corporate environment exposes students to the attacker's way of thinking when targets a corporate environment. Section 5 Log Management focuses on how log management can be used to mitigate risks. Section 6 Why is SIEM necessary? presents the reasons why data breaches are increased and how SIEM can be of an assistance. Section 7 Use Cases for SIEM helps on how to organize and prioritize use cases effectively. Section 8 Elements of SIEM introduces Big 3, Process flow, Features, Event life cycle, SOC controls and mgmt., SIEM architecture, Dashboards and Use cases. Section 9 SIEM deployment Options describes SIEM deployment options as self-hosted, self-managed to Hybrid-model, Jointly-managed. Section 10 incorporates a SIEM Essentials Quiz, section 11 Splunk presents Splunk's user interface and all its features. And finally, sections 12-18 teach students basic transforming commands and how to create reports and dashboards.

A Guide to Ransomware Protection is a 2-hour course which exposes students to ransomware measures and incident handling. The course is consisted of 7 sections, the first one introduces ransomware to students, describes the history of ransomware as well as its dangers and impact. Then the types of ransomware are presented as crypto ransomware, ransomware as a service and mobile ransomware, with examples included. The section Modus Operandi focuses on how ransomware works, how they infect, how they make things inaccessible and presents bypass technique, anonymity and hiding. The precautionary and preventive measures section includes, among others, technical, administrative and management precautions. In addition, the course teaches students how to prepare against ransomware attacks and how to handle ransomware incidents.

Threat Modeling is a 5,5-hour course that includes terminology, tools, processes, supplementary, techniques, applied examples and countermeasures. The students in the Basics and Terminology section will learn about asset types, attack vector, attack surface, attack tree and attack life cycle. The Threat Modeling Tools and Techniques section targets on threat modeling tools, STRIDE methodology, DREAD methodology, TRIKE thread modeling tool, elevation privilege threat modeling tool, Delphi technique, common mistakes and correct questions and multilevel threat modeling. In the Microsoft Threat Modeling Tool In-Depth section Microsoft threat modeling installation is analyzed as well as the usage, templates and modifications. Students learn Microsoft SDL basics, resources, Microsoft SDL for Agile projects in the next section and about threat catalogs: ENISA threat catalog and NIST threat catalog Attack Lifecycle Associated Threating and Threat Sources and Their Motivations in the section

Standards, Dictionaries and Other Useful Information. threat modeling approach. The last section is about countermeasures and how to choose the correct ones. It includes exercises and the NIST Data Centric Threat Modeling Approach and Activity.

Regarding the "Purple Team" category, Python: Digital Forensics & Binary Exploits with Python is a 6 hour course which aims to solve real-world forensics problems with innovative solutions by teaching students about network forensics, using tools to obtain and analyze volatile memory images, removing unwanted code and adding Trojan code, analyzing simple Linux executable files and modifying them using the gdb debugger, investigating Windows and GNU/Linux environments, using Python to complete enumeration, exploitation, and data exfiltration and analyzing Windows executable files and modifying them using the Immunity Debugger. The course consists of two sections: Python Digital Forensics and Binary Exploits with Python. The first section exposes students to network forensics and how to read, sort, sniff raw packets and analyze network traffic, analyze volatile memory. In addition, the course introduces tools used for obtaining and analyzing volatile memory images. The second section introduces binary exploits used to bypass password or product key tests and add Trojan code as well as teaches how to find vulnerabilities, analyze a crash in a debugger, create a crafted attack, and achieve remote code execution on Windows and Linux.

Wireless Hacking and Security is a 9-hour course which demonstrates wireless attacks and techniques used to defend the network. Apart from basic wireless network security concepts, the course introduces how to secure desktop clients, including legacy clients, Windows 7 and 8, Linux clients, as well as physical security and security policies enforcement, how to secure Wireless Access Points, smartphones, tables, WiMAX, ZigBee, RFID, and Bluetooth. Then the course focuses on hacking wireless devices, presents the hacking basics, as penetration testing methodology and tools used for hacking wireless devices and demonstrates a number of attacks on wireless devices. The course ends with a section regarding wireless security best practices which include the network design, the wireless clients and access points configuration, corporate policies and security testing.

Hacking and Securing Kubernetes Clusters is a 4-hour course that teaches how to attack and defend Kubernetes clusters. In this course students learn about Kubernetes Fundamentals, the common Kubernetes terms, Kubernetes components, deploying the vulnerable application and they are presented of an introduction to Kubectl. In addition, students are taught about the Kubernetes attack surface, how a misconfigured Kubernetes Cluster can be exploited by attackers, how to attack the API Server using insecure port, how to attack a misconfigured Kubelet API and how exposed Kubernetes Dashboard can be abused. The course also includes Static Analysis of YAML files using Kube-audit and Kubesec, security assessments using Kube-hunter, cluster audits using Kube-bench and Docker images scan using trivy. Regarding the defenses of Kubernetes Clusters, the course focuses on the limitation of network exposure, authorization, Kubernetes Secrets, admission controllers and how network policies limit the attack surface. Finally, the use Kubernetes Security Context to prevent attacks is presented.

Practical Cyber Threat Hunting is an 8.5-hour course which consists of 4 sections. The first one is an introduction to threat hunting and a presentation of incident response steps. In particular, the instructor creates a real-life attack scenario in a demo lab and presents threat intelligence sources and types, basic definition and terms like IOC, TTP, Cyber Kill Chain Model. The section Network Forensic and Pcap Analysis for threat hunters focuses on phishing detection over SMTP and DNS traffic, understanding protocol anomalies, detecting anormal user agents and analyzing ransomware traffic. In addition, buffer overflow exploit detection over the network is presented, as well as SSH tunnel traffic analysis, ICMP tunnel analysis, DNS tunnel analysis, tunnel techniques for detecting pivoting. SQL injection analysis from network traffic, detecting command injection attacks with network forensic, web shell detection with Pcap analysis, file upload attacks analysis, RFI And LFI attack detection with network hunting and XSS attack analysis with Pcap are also demonstrated in this section. The course's next section is Memory Forensic for threat hunters which starts with an introduction to memory forensics, Windows internals & fundamental Windows processes as well as process injection, process hollowing detection techniques, thread injection and PE injection detection techniques. ZEUS botnet malware memory dump analysis, DLL injection memory analysis, Stuxnet memory analysis, DarkComet Rat memory analysis and Cridex rat memory analysis are topics also covered in this section. The final section of this course is Endpoint analysis for threat hunters demonstrates threat hunting over ELK. The instructor explains event id numbers which are used for threat hunting, analyzes a real-life scenario, detects malicious word documents, hta files, unsigned exe files, vbs files and others. Ways to detect and investigate tunneling methods are also presented, as well as how to map attacks using MITRE framework. The course continues with incident response with Google Rapid and Osquery, threat hunting with virus total intelligence platform, APT attack simulation in a demo network & cyber kill chain and concludes with a research over security devices for detection and preventing.

Kali Linux: Network Scanning, Pentesting & Digital Forensic is a 9-hour course divided in 3 sections. The first one, Digital Forensics with Kali Linux, presents a brief introduction to digital forensics and forensic imaging and teaches how to use dc3dd tool to acquire images from hard drives, mobile devices, thumb drives, or memory cards. In addition, the Autopsy forensic suite and other specialized tools, such as the Sleuth Kit and RegRipper are introduced, which are used to extract and analyze various artifacts from a Windows image. The course also teaches how to perform analysis of an Android device image using Autopsy, about file carving and recovery of deleted data, and the process of acquiring and analyzing RAM memory (live analysis) using the Volatility framework. Lastly, the course target on how to report and present digital evidence found during the analysis. The section Finding and Exploiting Hidden Vulnerabilities focuses on vulnerability assessments and in particular the process of VAPT (Vulnerability Assessment and Penetration Testing) using Nessus and OpenVas. The course also teaches how to use Metasploit to exploit vulnerabilities and how to document a penetration test report. The final section, Mastering Kali Linux Network Scanning, focuses on the use of Kali Linux to gain control over a network using discovery scanning, port scanning, service enumeration, operating system identification and vulnerability mapping. Network traffic capture and analysis along with leveraging

OpenVAS 9 for vulnerability scanning is also presented as well as how to create packages and host custom repositories along with securing and monitoring Kali Linux at the Network and filesystem level.

2.2.3. Certifications

141 cybersecurity related certifications from were reviewed for the purpose of this dissertation. Each certification was classified based on its content in "Red Team", "Blue Team" and "Purple Team" categories. The detailed results can be found in the following link and the aggregated results are presented in the table below:

Table 3. Certifications Categorization Results

Category	Count of Modules
Red Team	59
Blue Team	79
Purple Team	3

According to research results, 59 certifications were classified as "Red Team", meaning that the main focus was on practical attacking concepts. Indicative certifications that were integrated in this category are:

- EC Council's Certified Ethical Hacker (CEH),
- GXPN: GIAC Exploit Researcher and Advanced Penetration Tester,
- Offensive Security Certified Professional (OSCP),
- eLearnSecurity Certified eXploit Developer eCXD,
- Pentester Academy's Certified Red Teaming Expert,
- Certified Penetration Testing Engineer C)PTE,
- CREST Certified Malware Reverse Engineer (CCMRE),
- eLearnSecurity Web application Penetration Tester eXtreme eWPTXv2,
- CompTIA Pentest+.

79 certifications were classified as "Blue Team", meaning that the main focus was on practical defensing concepts. Indicative certifications that were integrated in this category are:

- EC-Council's Certified Incident Handler (ECIH),
- GCDA: GIAC Certified Detection Analyst,
- Security Blue Team's Blue Team Level 1 (BTL1),
- eLearnSecurity Certified Digital Forensics Professional eCDFP,
- eLearnSecurity Certified Threat Hunting Professional eCTHP,
- GCFA: GIAC Certified Forensic Analyst,
- GCED: GIAC Certified Enterprise Defender,
- Certified Network Defender CND,

- CREST Practitioner Intrusion Analyst CPIA,
- CREST Practitioner Threat Intelligence Analyst (CPTIA),
- CyberSec First Responder CFR,
- IBM Certified SOC Analyst - IBM QRadar SIEM V7.3.2.

3 certifications were classified as “Purple Team”, meaning that the main focus was on practical defensing and attacking concepts. The certifications that were integrated in this category are:

- GDAT: GIAC Defending Advanced Threats,
- GCIH: GIAC Certified Incident Handler,
- GREM: GIAC Reverse Engineering Malware.

Analyzing the “Red Team” certifications, EC-Council’s Certified Ethical Hacker (CEH), one of the most well-known and in demand certification, teaches the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization. The course consists of 20 modules:

- Module 01: Introduction to Ethical Hacking,
- Module 02: Footprinting and Reconnaissance,
- Module 03: Scanning Networks,
- Module 04: Enumeration,
- Module 05: Vulnerability Analysis,
- Module 06: System Hacking,
- Module 07: Malware Threats,
- Module 08: Sniffing,
- Module 09: Social Engineering,
- Module 10: Denial-of-Service,
- Module 11: Session Hijacking,
- Module 12: Evading IDS, Firewalls, and Honeypots,
- Module 13: Hacking Web Servers,
- Module 14: Hacking Web Applications,
- Module 15: SQL Injection,
- Module 16: Hacking Wireless Networks,
- Module 17: Hacking Mobile Platforms,
- Module 18: IoT Hacking,
- Module 19: Cloud Computing,
- Module 20: Cryptography.

The training option vary between self-study, online training, master class, training partner and education partner. The certification exam is a 4-hour exam with 125 multiple choice questions. Break-the-code challenge is introduced with CEH v11, and includes 24 hacking challenges across 4 levels of complexity that cover 18 attack vectors, including the OWASP Top 10.

Global Information Assurance Certification’s GXPN: GIAC Exploit Researcher and Advanced Penetration Tester certification focuses on how to find and mitigate

significant security flaws in systems and networks, how to conduct penetration tests, how to model the behavior of attackers to improve system security and finally how to demonstrate the business risk associated with these behaviors. The areas covered in the certification are Network Attacks, Crypto, Network Booting, Restricted Environments, Python, Scapy, Fuzzing and Exploiting Windows and Linux Penetration Testers. In particular, the topic areas for each exam part are the following:

- Accessing the Network,
- Advanced Fuzzing Techniques,
- Advanced Stack Smashing,
- Client Exploitation and Escape,
- Crypto for Pen Testers,
- Exploiting the Network,
- Fuzzing Introduction and Operation,
- Introduction to Memory and Dynamic Linux Memory,
- Introduction to Windows Exploitation,
- Manipulating the Network,
- Python and Scapy For Pen Testers,
- Shellcode,
- Smashing the Stack,
- Windows Overflows.

No specific training is required for this certification, however, a variety of training sessions are available. The certification exam is 3 hours in length and consists of 55-75 questions.

Offensive Security Certified Professional (OSCP) certification is a well-known penetration testing certification that consists of several target machines that must be compromised and a report describing the exploitation process for each target. The examinees have 23 hours and 45 minutes to complete the challenge itself and a further 24 hours to submit the documentation. The Penetration Testing with Kali Linux (PEN-200) course is required prior the certification exam and it analyzes penetration testing tools and techniques via hands-on experience on using a virtual lab environment.

The topics covered in the course are the following:

- Penetration Testing: What You Should Know
- Getting Comfortable with Kali Linux
- Command Line Fun
- Practical Tools
- Bash Scripting
- Passive Information Gathering
- Active Information Gathering
- Vulnerability Scanning
- Web Application Attacks
- Introduction to Buffer Overflows
- Windows Buffer Overflows

- Linux Buffer Overflows
- Client-Side Attacks
- Locating Public Exploits
- Fixing Exploits
- File Transfers
- Antivirus Evasion
- Privilege Escalation
- Password Attacks
- Port Redirection and Tunneling
- Active Directory Attacks
- The Metasploit Framework
- PowerShell Empire
- Assembling the Pieces: Penetration Test Breakdown
- Trying Harder: The labs.

This course and certification equip the students with the ability to use information gathering techniques to identify and enumerate targets running various operating systems and services, write basic scripts and tools for the penetration testing process, analyze, rectify, adjust, cross-compile, and port public exploit code, conduct remote, local privilege escalation, and client-side attacks, identify and exploit XSS, SQL injection, and file inclusion vulnerabilities in web applications, leverage tunneling techniques to pivot between networks.

eLearnSecurity Certified eXploit Developer eCXD certification focuses on Windows and Linux exploit development and software vulnerability identification in general. The areas covered in this certification are:

- Windows and Linux internals
- Reverse engineering (x86 and x64 platforms)
- Software debugging
- Shellcoding
- Windows and Linux exploit development (including scripting knowledge)
- Bypassing modern anti-exploit mechanisms (ASLR/PIE, Stack Cookie, NX/DEP, RELRO etc.)
- Exploiting hardened hosts and overcoming limitations

No specific training is required for this certification, however, INE's Exploit Development Student learning path is recommended as training course as it provides theoretical and hands-on practical sessions. The certification exam consists of a software vulnerability identification and exploitation against actual Windows and Linux software which are protected by multiple anti-exploit mechanisms, hardened hosts and other limitations. In addition, the examinees are expected to recommend alternative exploitation paths. The exam is performed in a real-world virtual lab environment. The students are also required to submit a report documenting findings and observations and recommending remediation actions within 14 days.

Pentester Academy's Certified Red Teaming Expert certification focuses on solving practical and realistic challenges in fully patched Windows infrastructure labs

containing multiple Windows domains and forests. This certification validates the ability to assess the security of an enterprise Windows infrastructure with multiple domains and forests by abusing the functionality and trusts. More specifically, the topics covered are the following:

- Active Directory Enumeration,
- Abusing built-in functionality for code execution,
- Local Privilege Escalation,
- Credentials Replay,
- Using administration tools to compromise other machines,
- Bypassing countermeasures like Application White-listing and anti-virus,
- Pivot through windows machines to bypass Firewall rules,
- Domain Privilege Escalation using Kerberoast, Kerberos delegation, Abusing protected groups, abusing enterprise applications and more,
- Domain Persistence and Dominance using Golden and Silver ticket, Skeleton key, DSRM abuse, AdminSDHolder, DCSync, ACLs abuse, host security descriptors and more,
- Forest privilege escalation using cross trust attacks,
- Inter-forest trust attacks,
- Abusing SQL Server Trusts,
- Lateral movement and hunting for business secrets using built-in Windows tools.

The students have 48 hours to complete the hands-on certification exam and it is required to submit a report documenting the solutions and mitigations.

The Windows Red Team Lab offers the capability to practice attacks against Windows network infrastructure and Active Directory starting as a non-admin user move so as to gain admin access to multiple forests by exploiting domain features and vulnerabilities. In addition, the Red Team Exercises provides 42 challenges which require 60 flags to be captured. There are 8 sections, Section 1: Abuse Applications, Impersonate Users, Escalate Privileges which teaches domain enumeration, Single sign-on in Active Directory, privilege escalation in enterprise applications, abusing built-in functionality for code execution, local privileges escalation on Windows, credential replay, domain privileges abuse, offline brute force attack against domain objects. Section 2: Gain Admin Privileges, Defeat Countermeasures and Restrictions, Hunt for Domain Privileges, Escalate which teaches domain enumeration, situation awareness on foothold machine, extracting credentials from Windows machine, credential replay, domain privileges abuse. Section 3: Pivot through Machines, Defeat Countermeasures, Abuse Kerberos, Exfiltrate Juicy Data which teaches using administration tools to compromise other machines, pivot through machines, Kerberos functionality abuse, using administration tools to access data from databases, search interesting data in databases. Section 4: Pivot through Machines and Forest Trusts, Low Privilege Exploitation of Forests, Capture Flags and Database which teaches trust abuse in databases, pivot through forests, built-in tools for command execution, using administration tools to access data from databases and search interesting data in databases. Section 5: Enumerate Users and Emails, Create Emails, Custom Payloads, Exploit End-User Machines which teaches to create emails with weaponized

attachments, craft payloads which provide code execution, utilize available information to chain attacks, bypass countermeasures, find privileges in domain. Section 6: Compromise Applications, Achieve Command Execution, Impersonate Users, Move Laterally, Escalate Privileges which teaches abusing functionality of enterprise applications, using architecture specific payloads, user impersonation, user hunting for high privileges, dumping system secrets, credential replay, lateral movement. Section 7: Obtain Domain Privileges, Compromise Forest which teaches how to abuse Kerberos functionality, understand and abuse intra-forest trust, understand and abuse various groups in root domain of forest. Finally, Section 8: Compromise a Forest from another Trusted Forest teaches about forest enumeration, abuse Kerberos functionality, understand and abuse inter-forest trust, using administrator tools for command execution.

Analyzing the "Blue Team" certifications, EC-Council's Certified Incident Handler (ECIH) focuses on experience regarding handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

The course outline includes:

- Introduction to Incident Handling and Response,
- Incident Handling and Response Process,
- Forensic Readiness and First Response,
- Handling and Responding to Malware Incidents,
- Handling and Responding to Email Security Incidents,
- Handling and Responding to Network Security Incidents,
- Handling and Responding to Web Application Security Incidents,
- Handling and Responding to Cloud Security Incidents,
- Handling and Responding to Insider Threats.

The certification requires a 3-day training program or 24 hours total class time which includes hands-on labs followed by a 3-hour exam of 100 multiple choice questions.

Global Information Assurance Certification's GCDA: GIAC Certified Detection Analyst certification target on the collection, analysis and the use of network and endpoint data sources to detect malicious or unauthorized activity by using Security Information and Event Management tools among others. The certification covers SIEM Architecture and SOF-ELK, Service Profiling, Advanced Endpoint Analytics, Baselining and User Behavior Monitoring, Tactical SIEM Detection and Post-Mortem Analysis. In particular, the topic areas for each exam part are the following:

- Alert Analysis,
- Device Discovery,
- Endpoint Logging Analysis,
- Endpoint Logging Collection,
- Log Aggregation and Parsing,
- Log Collection,
- Log Output and Storage,
- Network Service Log Analysis,

- Network Service Log Collection & Enrichment,
- Post-Mortem Analysis,
- Software Monitoring,
- User Monitoring.

No specific training is required for this certification, however, a variety of training sessions are available. The certification exam is 2 hours in length and consists of 75 questions.

Security Blue Team's Blue Team Level 1 (BTL1) certification demonstrates the ability to defend networks and systems from cyber threats. The course supporting the certification consists of 6 domains: Domain 1 – Security Fundamentals, Domain 2 – Phishing Analysis, Domain 3 – Threat Intelligence, Domain 4 – Digital Forensics, Domain 5 – SIEM and Domain 6 – Incident Response. More specifically:

- Domain 1 – Security Fundamentals offers an introduction to security fundamentals, focuses on soft skills and networking and presents security controls and management principles.
- Domain 2 – Phishing Analysis presents an introduction to e-mails and phishing, introduces types of phishing e-mails, demonstrates tactics and techniques that are used in phishing attacks, teaches about analyzing URLs, attachments, and artifacts, taking defensive measures and how to document the investigation report. This section also includes a phishing report challenge.
- Domain 3 – Threat Intelligence targets on core intelligence concepts starting with an introduction to threat intelligence and an analysis on threat actors and Advanced Persistent Threats. It focuses on operational, tactical and strategic threat intelligence and presents malware and global campaigns.
- Domain 4 – Digital Forensics introduces digital forensics and presents forensics fundamentals. This sections teaches students regarding digital evidence collection and Windows and Linux investigations. Volatility and Autopsy tools are covered so as to enable students to learn more about files, browsing history, and memory dumps to build up a timeline of events.
- Domain 5 – SIEM targets on how to conduct log analysis and investigate security events and incidents. In particular, students are introduced to SIEM and topics as logging, aggregation and correlation are analyzed. This section focuses on the use of Splunk SIEM and presents its features.
- Domain 6 – Incident Response is the final section and provides an introduction to incident response and teaches the three phases of an attack handling: the preparation phase, the detection and analysis phase and the containment, eradication, and recovery phase. This section also targets on how to use the MITRE ATT&CK knowledge base as a leverage to respond to malicious attacks.

The certification process consists of a 24-hour incident response exam conducted on a cloud lab via an in-browser session for up to 12 hours. As the certification requires a respective report, students can use the remaining 12 hours in order to document their actions and findings.

eLearnSecurity Certified Digital Forensics Professional eCDFP certification focuses on proving the technical digital forensics expertise of the student. The areas covered by this certification are the following:

- File & disk analysis
- Windows forensics
- Network forensics
- Log analysis
- Timeline analysis
- In-depth knowledge of file systems and tools such as WinHex, regripper, tcpdump etc.

The skills taught within the Digital Forensics Professional learning path are: letters of engagement and the basics related to a forensic investigation engagement, networking concepts, digital forensics processes and methodologies, proficiency in file & disk analysis, analyzing Windows artifacts, analyzing traffic capture files, file systems and disk editors, constructing actionable timelines, proficiency in log analysis, manual intrusion detection skills using the established forensics-related toolkit and correlating data from various sources.

No specific training is required for this certification, however, INE's Digital Forensics Professional (DFP) path is recommended as training course as it provides theoretical and hands-on practical sessions. The certification exam targets on the evaluation of the ability to use a variety of forensic techniques, inside a fully featured and real-world environment. The exam is performed in a real-world virtual lab environment and students are expected to complete a real-world simulation based on actual scenarios and incidents.

eLearnSecurity Certified Threat Hunting Professional eCTHP certification proves one's threat hunting and threat identification capabilities. The areas covered by this certification are the following:

- Network packet/traffic analysis
- Data enrichment with Threat Intelligence
- Data correlation
- In-depth knowledge of tools such as Wireshark, Redline & IOC editor
- IOC-based threat hunting
- Memory analysis/forensics
- Windows/Linux event analysis
- Log analysis
- Detection of any stage of the "Cyber Kill Chain" (Information Gathering, Exploitation, Post-exploitation).

The skills that are taught in the context of the certification are: letter of engagement and the basics related to a threat hunting engagement, advanced networking concepts, threat hunting processes and methodologies, packet/traffic analysis, enriching data with threat intelligence, familiarly with tools such as Wireshark, redline, ioc editor, Sysmon & volatility, how to detect all stages of the "cyber kill chain", familiarity with ioc-based

hunting, ability in analyzing memory dumps, good understanding of windows events, ability in analyzing logs, manual threat detection through process analysis and ability in correlating data from various sources.

No specific training is required for this certification, however, INE's Threat Hunting Professional path is recommended as training course as it improves knowledge and skills. The certification exam targets on the performance of an actual threat hunt on a corporate network and is modeled after real-world scenarios and cutting-edge malware. The students are required to submit a documented report including their observations and finding, recommending mitigating actions and propose defense strategies within 14 days.

Regarding "Purple Team" certifications, Global Information Assurance Certification's GDAT: GIAC Defending Advanced Threats certification focuses on "how adversaries are penetrating networks, but also what security controls are effective to stop them". The area covered are: advanced persistent threat models and methods, detecting and preventing payload deliveries, exploitation, and post-exploitation activities, using cyber deception to gain intelligence for threat hunting and incident response.

The topic areas for each exam part are the following:

- Command and Control With Exfiltration Fundamentals,
- Controlling scripts in the enterprise,
- Controls for Detecting and Preventing Payload Delivery to End Users,
- Current Threat and Attack Landscape Along the APT Attack Cycle Outline,
- Defining Rules and Visualizing Results,
- Detecting and Preventing C2 and Exfiltration,
- Detecting and Preventing Installation,
- Detecting and Preventing Lateral Movement,
- Endpoint Protection,
- Introduction to Post Event Activities,
- Learning Internal Networks and Conceptualizing Defensible Architectures,
- Leveraging Cyber Deception to Inform Threat Intelligence for Threat Hunting,
- Phases of the Software Development Lifecycle,
- Software Attacks and Mitigations.

No specific training is required for this certification, however, a variety of training sessions are available. The certification exam is 2 hours in length and consists of 75 questions.

Global Information Assurance Certification's GCIH: GIAC Certified Incident Handler certification focuses on detecting, responding and resolving computer security incidents by using specific tools. The areas covered in this certification are: Incident Handling and Computer Crime Investigation, Computer and Network Hacker Exploits and Hacker Tools (Nmap, Nessus, Metasploit and Netcat). In particular, the topic areas for each exam part are the following:

- Covering Tracks on Hosts,
- Covering Tracks on the Network,

- Domain Attacks,
- Drive-By Attacks,
- Endpoint Attacks and Pivoting,
- Incident Handling and Digital Investigations,
- Memory and Malware Investigations,
- Metasploit,
- Netcat,
- Network Investigations,
- Password Attacks,
- Physical Access Attacks,
- Reconnaissance and Open-Source Intelligence,
- Scanning and Mapping,
- SMB Scanning,
- Web App Attacks.

No specific training is required for this certification, however, a variety of training sessions are available. The certification exam is 4 hours in length and consists of 100-150 questions.

Global Information Assurance Certification's GREM: GIAC Reverse Engineering Malware certification is addressed to professionals who protect organizations from malicious code and it focuses on knowledge and skills to reverse-engineer malicious software targeting Microsoft Windows and web browsers etc., forensic investigations, incident response, and Windows system administration. The main areas that are covered in this certification are: analysis of malicious document files, analysis of protected executables, analysis of web-based malware, in-depth analysis of malicious browser scripts and in-depth analysis of malicious executables, malware analysis using memory forensics and malware code and behavioral analysis fundamentals, Windows assembly code concepts for reverse-engineering and common Windows malware characteristics in assembly. Regarding the certification's objectives, the topic areas for each exam part are the following:

- Analysis of Malicious Document Files,
- Analyzing Protected Executables,
- Analyzing Web-Based Malware,
- Common Windows Malware Characteristics in Assembly,
- In-Depth Analysis of Malicious Browser Scripts,
- In-Depth Analysis of Malicious Executables,
- Malware Analysis Using Memory Forensics,
- Malware Code and Behavioral Analysis Fundamentals,
- Windows Assembly Code Concepts for Reverse-Engineering.

No specific training is required for this certification, however, a variety of training sessions are available. The certification exam is 2 hours in length and consists of 75 questions.

3. Conclusion

The results demonstrate that Master's Degrees focus more on "Generic" courses, less on "Blue Team" courses and even less on "Red Team" courses. The Udemy platform focuses more on "Red Team" courses, less on "Blue Team" courses and even less on "Purple Team" courses. Finally, the available certifications focus more on "Blue Team" knowledge, less on "Red Team" and much less on "Purple Team".

The results might suggest that as the master's degrees are academic degrees earned from an educational institution, either national or private, which in general offer a more theoretical foundation and focus more on introducing the basic concepts to students and set the base of further education, their courses target mostly on providing general knowledge regarding cybersecurity. In addition, as Red Team concepts and techniques include an offensive thought process, they teach how to think as an attacker, universities may not prefer to promote such skills and that may be the reason why the Red Team courses are the fewest among all modules. Although master's degrees are not addressed exclusively to younger students, it is possible that some of them may try offensive practices in real-world environment. In other words, the ethical considerations of teaches students how to hack systems, even from an ethical point of view may act as an inhibitor for including Red Team courses to master's degree's curriculum.

On the other hand, regarding the Udemy courses results, it is important to mention that a Udemy course can be created and uploaded by any instructor free of charge and that the platform offers the option of charging students to attend the course. Having said that, the Udemy courses reflect the topics that the instructors, which are part of the cybersecurity community and are usually cybersecurity professionals consider as the most attractive and will draw the attention of most students. The Udemy students may be either cybersecurity professionals or professionals from related or unrelated industries that want to expand their knowledge, shift to cybersecurity or are interested in the field. Moreover, a Udemy course's duration is less than the duration of a master's degree, requires less commitment and has a lower prize. Considering all the above and in correlation with the research results that showed that the Red Team courses are more than double than the Blue Team courses, it may be concluded that offense is more interesting to the cybersecurity community and topics as ethical hacking and malware development are significantly more appealing.

The cybersecurity certifications teach, assess and accredit practical skills that can promptly be used in action. Students choose to obtain a cybersecurity certification in order to validate their skills and attract more recruiters. In addition, a number of certifications are often required from employers or clients as proof of one's competency. By observing the research results we can ascertain that more "Blue Team" certifications are available than "Red Team". As this contradicts with the Udemy courses results, we may assume that the industry's and employers' requirement have shaped the certifications market. In addition, considering that certifications act as substitutes of academical education and, in some cases, work experience, we can notice that likewise the master's degrees results, the "Blue Team" certifications outnumber the "Red Team" ones.

An interesting remark is that, in all cases, “Purple Team” related courses are less preferred. More specifically, regarding the Udemy courses, it was noted that even the courses that were classified as “Purple Team”, they dedicate less time to the defense sections. This is may due to the fact that usually purple teams are not a specific team separate from red and blue teams, but more a function or methodology for the collaboration between the two teams in order to maximize the efficiency and succeed the optimal level of security.

While the language barrier limits the generalizability of the results, as in all cases the processed data were only those available in English, this research which aimed to analyze the cybersecurity education curriculum has shown the focus of schooling and training regarding the preferred approach to cybersecurity and has pointed out that the different examined pillars prioritize different content.

References

[1] M. C. Crichlow, "A Study on Blue Team’s OPSEC Failures," University of Twente, 2020.

[2] M. Andreolini, V. G. Colacino, M. Colajanni and M. Marchetti, "A Framework for the Evaluation of Trainee Performance in Cyber Range Exercises," Springer Science+Business Media, LLC, part of Springer Nature, 2019.

[3] S. Bruskin, P. Zilberman, R. Puzis and S. Shwarz, "SoK: A Survey of Open Source Threat Emulators," 2020.

[4] M. M. Yamin, B. Katt and V. Gkioulos, "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools," Computers & Security, 2019.